ACCEPTED MANUSCRIPT

# Design, Implementation, and Evaluation of a Fingerprint-Based Ignition Key for Motorcycles

**Heru Supriyono[1*], Anugrah Adi Wijayanto[1], Rozita Jailani[2], Mohammad Osman Tokhi[3]**

[1]Department of Electrical Engineering, Universitas Muhammadiyah Surakarta, 57102, Indonesia
[2]Department of Electrical Engineering, University Teknologi MARA, Selangor, 40450, Malaysia
[3]Division of Electrical and Electronic Engineering, London South Bank University, London, SE1 0AA, UK

Email: Heru.Supriyono@ums.ac.id

**Abstract**

Cases of motorcycle theft by breaking mechanical key are still a serious problem in some countries. Therefore, this article discusses the process of development, implementation, and evaluation of a fingerprint-based ignition key for motorcycles. To prevent theft, a motorcycle can only be turned on by a registered fingerprint, and an alarm will ring if the sensor receives an unregistered fingerprint. This prototype used the main component of the SEN0188 fingerprint sensor, Arduino Uno microcontroller, LM317 voltage regulator, and the buzzer alarm module. The test results in shaded place showed that the proposed key successfully ignited the engine by 80% with a dry and clean thumb. However, if the thumb is oily or dirty, the success scanning rate is only 36% of 25 attempts. The proposed key also successfully activates a warning alarm if a fingerprint scan attempt fails three times in a row. Test results on potholes, bumpy, dusty, and puddles roads indicate that no hardware has been disturbed or damaged. Therefore, this prototype has the potential to be further developed and implemented on a large scale in an effort to reduce motorcycle theft rates.

Keywords: Motorcycle, Biometric key; Fingerprint key; Arduino Uno

## 1. Introduction

Motorcycle theft is still a major criminal problem in several countries. Economic factors and unemployment are thought to be the main causes of these massive cases. In 2018, based on 2019 criminal statistics, cases of motor vehicle theft in Indonesia was in second-ranked with 27731 cases [1]. Similar cases have also been reported in Nigeria, the Philippines, Malaysia [2]–[4].

Older generations of motorcycles use mechanical keys, which are physical keys that must be inserted into a keyhole then rotated clockwise in “on” position, and then the motorcycle engine can be turned on either using an electric starter button or using a kick starter. To turn off the engine, from the “on” position, the key has to be turned counter-clockwise until the “off” position so that the engine will turn off. In addition to turning on and off the engine, the mechanical key on the motorcycle also serves to lock the handlebar.

The disadvantage of the mechanical key is that they can be tampered by a mock mechanical key commonly referred to as a T-shaped key. In the case of motorcycle theft, the thief frequently uses the T-shaped key to damage the mechanical key to turn on the engine. From the information obtained from the mass media, it can be noted that motorcycle theft is still a serious problem. Theft can occur in various places, such as in parking lots, in the yard, in boarding houses, offices, and so on.

The use of electronic systems to enhance safety and security in a broad perspective on various types of motorized vehicles attracts interest from researchers. The electronic system was proposed for tracking position and speed monitoring on vehicles such as a truck [5] where the system was equipped with a short message service (SMS) based notification if the vehicle is traveling above the predetermined maximum speed limit. A similar system but was more used to monitor the driver's driving style which was also equipped with an SMS notification if the vehicle speed exceeds the maximum speed limit proposed in [6]. With these systems, it was expected that the potential of vehicles in the event of an accident or endanger other vehicles would be reduced.

Efforts to improve motorized vehicle security that focuses on the theft also get the attention of researchers. For example, Singh [7] uses an electronic system based on a global positioning system (GPS) and cellular phone networks to track the vehicle when it is stolen or it an accident occurs so that it can easily be rediscovered. An anti-theft system uses GPS and SMS was also studied in [8] but with different features. A camera-based face recognition feature was implemented to the motorcycle which means the engine can only be turned on by people whose face data has been recorded in the camera.

The combination of camera, GPS, and SMS was also implemented in Pachica's study [9]. A camera was used to take a picture of the thief and in addition to receiving notifications that the motorcycle has been stolen, motorcycle owners can also turn off the engine remotely by cellular phone. Another variation of the anti-theft system for motor vehicles was the combination use of secondary keys based on radio frequency identification (RFID), alarms, and SMS as described in Jusoh study [10] where the system will turn on the alarm and send an SMS notification to the owner if someone tries to start the motorcycle without the appropriate RFID tag.

A biometric-based identification system is a system that is able to identify people based on the physical characteristics and behavior of that person [11]. The physical characteristics of people which can be used in biometric identification include the iris, face, hand finger geometry, and fingerprint, while the behavioral characteristics include voice, changes in signature patterns, and the habit of pressing buttons like on a keyboard. Fingerprint is a reliable technology with high accuracy in personal identification [12]. In addition, the use of fingerprints has advantages over the use of other technologies such as card or chip-based identification which involves using less material such as plastic or paper and also using less energy. Furthermore, when compared to password-based security or tokens or cards, fingerprint-based authentication has an advantage, because it's a part of the body.

The potential use of fingerprints for security systems is gaining attention from researchers. Fingerprint was proposed for controlling access to a limited area where the results of the research showed that the fingerprint was able to provide security protection at a good level [13]. Fingerprint was also used in intrusion detection system (IDS), which was to recognize whether the person has the right to access a computer system or not [14]. Fingerprint was also reported to have high accuracy in identifying personal when implemented in a management system in an organization [15].

Just like using other technologies, one of the concerns of widespread use of fingerprints in organizations or companies is privacy issues, such as by stealing fingerprint devices or servers or by copying the data [16]. In addition, another way of identity theft including fingerprint data is through a special program that decodes the fingerprint image file so that it can be used by others [17]. In general, to theft of physical infrastructure, security holes in the use of fingerprint for authentication systems include two main things, namely attacks on the system user interface and database [18]. However, with the improvement of the security gap, fingerprint technology is safe to use and it has high accuracy.

In many companies and agencies, fingerprint has been widely used to authenticate the presence of staff and workers [19]. Fingerprint was used to replace manual attendance systems because it was able to identify personalities more quickly and accurately. However, the use of fingerprint authentication for motorcycle security has not been widely reported by researchers, including in Indonesia. Thus, considering many advantages of fingerprint, its potential use for replacing the mechanical keys of motorcycles is considerably high. However, the problems arose including how to implement a fingerprint-based key system and how it performs. Therefore, this article discusses the process of designing, implementing, and testing the performance of a fingerprint-based ignition key system, where the fingerprint will be used as the primary key to replace the mechanical key and starter button of motorcycle.

## 2. Method

### 2.1. System Architecture

The overall system architecture is displayed in the block diagram in **Figure 1**. The proposed fingerprint-based key system requires a fingerprint sensor to read the fingerprint data of people who are allowed to turn on and turn off a motorcycle engine that must be registered first. The scanned fingerprint from the fingerprint sensor is then compared to the registered data list and its similarity status is sent to the microcontroller. Program in the microcontroller then read this similarity status, if the fingerprint data match, the microcontroller will generate a signal to turn on the relay module connected to the engine which replaced the mechanical key and the starter button, so that the electricity system and engine would be turned on. If there are certain number of fail attempts in a row, the microcontroller will generate a signal to turn on the alarm.

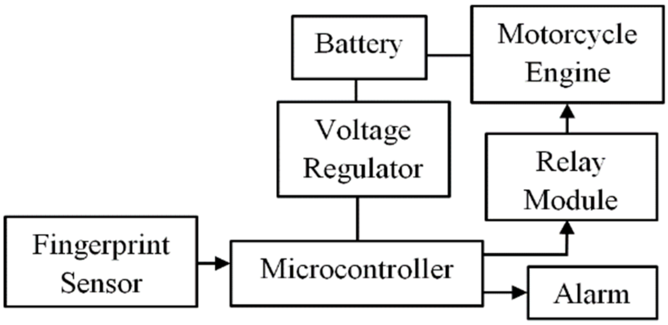


**Figure 1**. Block diagram representing proposed fingerprint-based key system architecture

Dfrobot SEN0188 commercial fingerprint sensor was used in the proposed system. It has the ability to scan and acquire the fingerprint image in less than one second and then store the acquired image to the internal memory/database which is able to store up to 1000 fingerprint images. This sensor requires voltage between 3.8 and 7.0 direct current volt (DCV) and works with typical operating current at 65 mA. The dfrobot SEN0188 sensor output was supplied to the Rev3 pin of Arduino Uno microcontroller. Arduino Uno was chosen because of its compatibility to dfrobot SEN0188 and its reliability when used in broad application by researchers involving on mobility environments for example in a wheeled robot [20] and in a portable machine for gas detection [21].

For relay module, on the input side, contains two relays that require a voltage of 5 DCV and current between 15 and 20 mA from the microcontroller while on the output side the relay module can accept a voltage of 250 alternating current volt (ACV) or 30 DCV with a current of 10A originating from the motorcycle battery. The alarm uses a buzzer module that works by using voltage between 4 and 8 DCV with current of less than 30mA connected to a microcontroller. For the microcontroller, the power was obtained from the motorcycle battery through an external power supply or voltage regulator.

The system architecture in this work is different from that reported by other researchers in the use of fingerprints for motorcycle security in [22], where the primary key to give the order to turn on or turn off the motorcycle engine was from Android smartphone while the fingerprint function just to enable command from Android smartphone.

### 2.2. Voltage regulator design

Power for the microcontroller could be provided using a dedicated external power supply or using an existing motorcycle battery. In this work, we decided to use the existing battery as a source of electricity for the microcontroller rather than using an external battery separately for stability reasons. The existing battery will always be charged when the engine is running. The 12 DCV existing battery needs to be reduced to 7 - 12 DCV to meet the specification of the Arduino Uno. Therefore, a regulator circuit was needed to reduce the voltage and current, as can be seen in Figure 2.

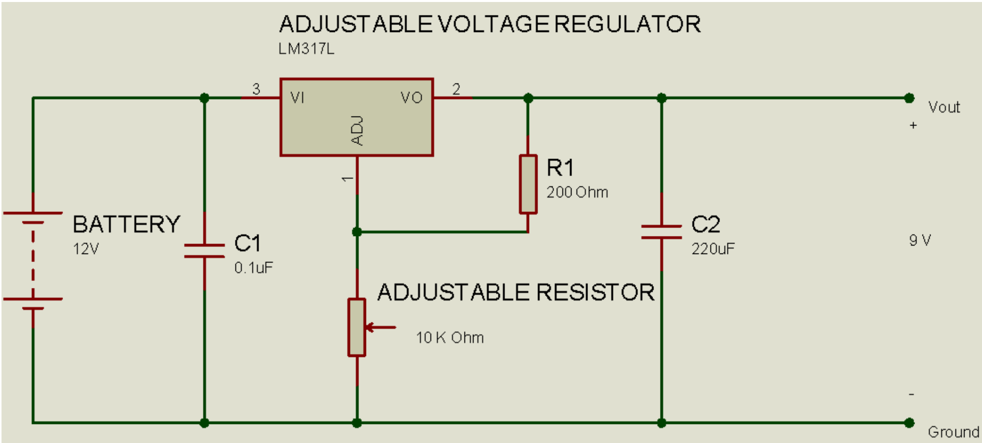


Figure 2. Voltage regulator circuit

The voltage regulator circuit used LM317 component, an adjustable power regulator that able to receive input power between 4.2 and 40 DCV and produces output between 1.2 and 37 DCV. The output voltage of the LM317 can be adjusted by changing the value of the adjustable resistor. In order to get a stable output voltage at a certain value, LM317 requires a minimum input voltage of 1.25 DCV higher than the expected output value with the smallest input value being 4.2 DCV. In the proposed system, the expected voltage regulator output is stable at 9 DCV to supply the Arduino Uno microcontroller.

### 2.3. Hardware design

The arrangement and connection of fingerprint-based key components is presented in Figure 3. The SEN0188 fingerprint sensor has 4 pins, i.e. vcc, ground, data transmitter (TD) and data receiver (RD) with the connection detail were as follow: vcc was connected to 5 DCV as a voltage source from Arduino Uno with red cable, ground was connected to ground pin of Arduino Uno with black cable, TD to send or output data was connected to pin 2 of Arduino Uno with white cable, and RD to receive data sent by TD was connected to pin 3 of Arduino Uno.

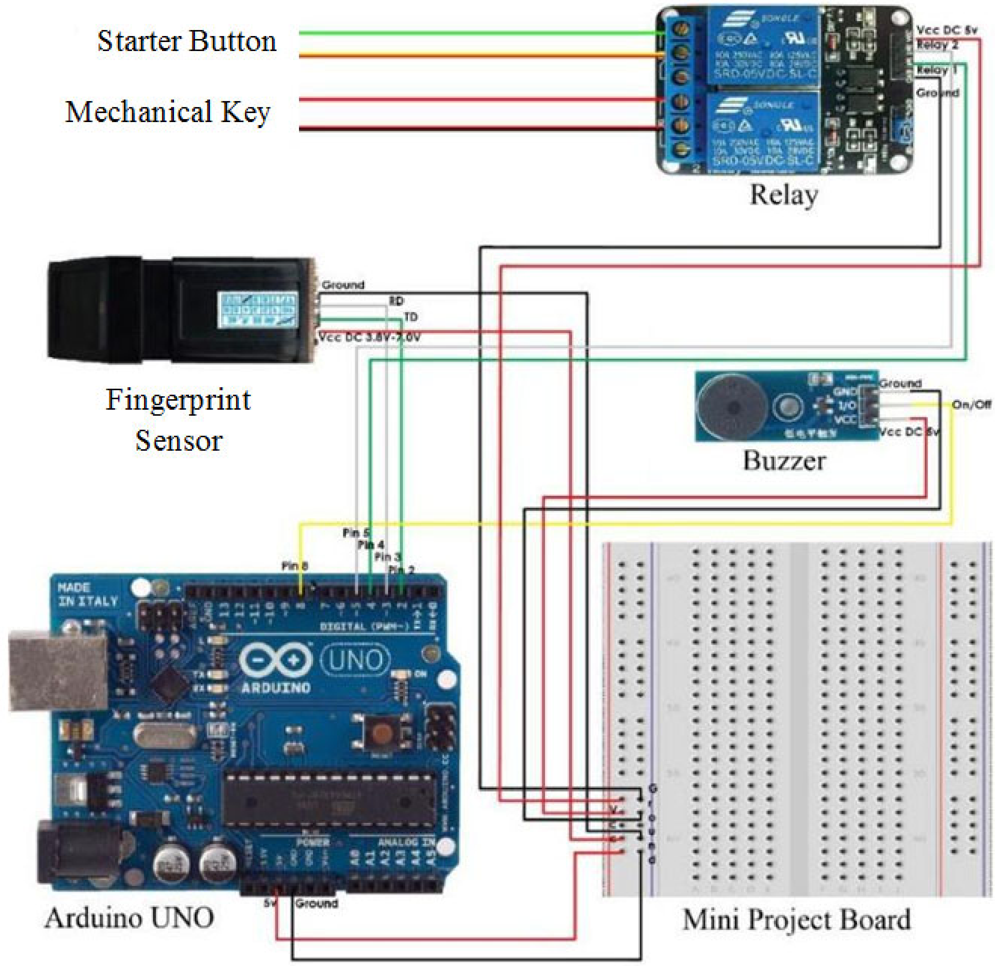


**Figure 3**. Wiring diagram of all components

The relay module has two relays, on the outside the relays were connected to the electrical path of the mechanical key (for relay 1) and the starter button (for relay 2) while the inside of the relay module has 4 pins with the technical connection were as follows: vcc with red wire was connected to the 5 DCV voltage source of Arduino, ground with black cable connected to Arduino Uno ground line, pin of relay 1 with green cable was connected to pin 4 of Arduino Uno and pin of relay 2 with white cable was connected to pin 5 of Arduino Uno. Then, in the buzzer module as an alarm there were 3 pins with the following connections: vcc with a red cable was connected to a 5 DCV voltage source of Arduino Uno, ground with a black cable was connected to the Arduino Uno ground line, and I/O line with yellow cable was connected to pin 8 of Arduino Uno as input for the buzzer module.

The hardware circuit has an on/off button switch to turn on and turn off the entire fingerprint-based key system. The entire set of hardware components, except the on/off switch and fingerprint sensor, were put in a plastic box so that they were protected from the risk of shock and pressure which can result in damage to the circuit when implemented on the motorcycle.

### 2.4. Software design

The main software developed in this fingerprint-based key was software on the Arduino Uno microcontroller. The software in the microcontroller processes the scanned fingerprint then uses it to ignite the engine. The processes of fingerprint registration and verification are presented in the flowchart in Figure 4 and Figure 5 respectively.

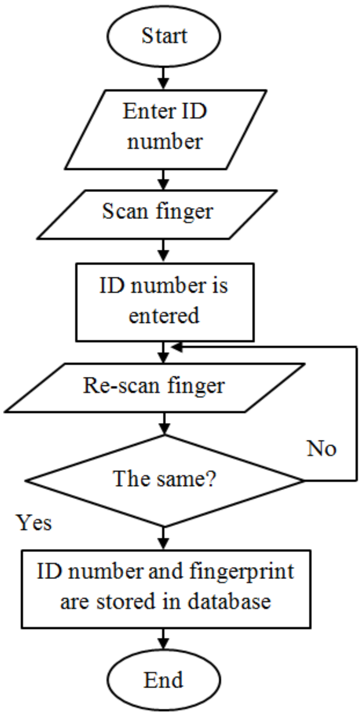


Figure 4. Flowchart of computation step for registering and recording fingerprint data

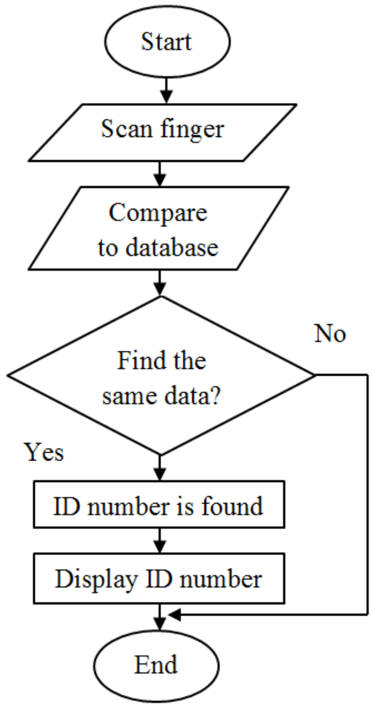


Figure 5. Flowchart of computation step for verifying fingerprint data

Figure 4 explains the process of registering and recording fingerprint identification (ID) number which will be stored in the memory/database. The first step is entering the ID number then selecting and scanning the fingerprint to be registered on the SEN0188 sensor so that the pair of ID numbers and the fingerprint image will be obtained. However, this data pair has not been stored in the database yet. The second stage is to re-scan the same fingerprint as was scanned in the previous stage. Then, the sensor compares whether the secondly-scanned fingerprint is the same as the firstly-scanned if the same then the pair of ID numbers and fingerprints will be stored in the database, otherwise, the sensor will ask to continue to repeat scanning until getting the same fingerprint as before.

Then, **Figure 5** explains the fingerprint verification process. The first step in the verification process is scanning the fingerprint in order to read and obtain the fingerprint image data. This data will be compared with the data stored in the database, if it matches one of the data in the database, the SEN0188 sensor will display its corresponding ID number, otherwise, no ID number would be displayed. Finally, the flow of computational steps of the overall program on the microcontroller is presented in **Figure 6**.

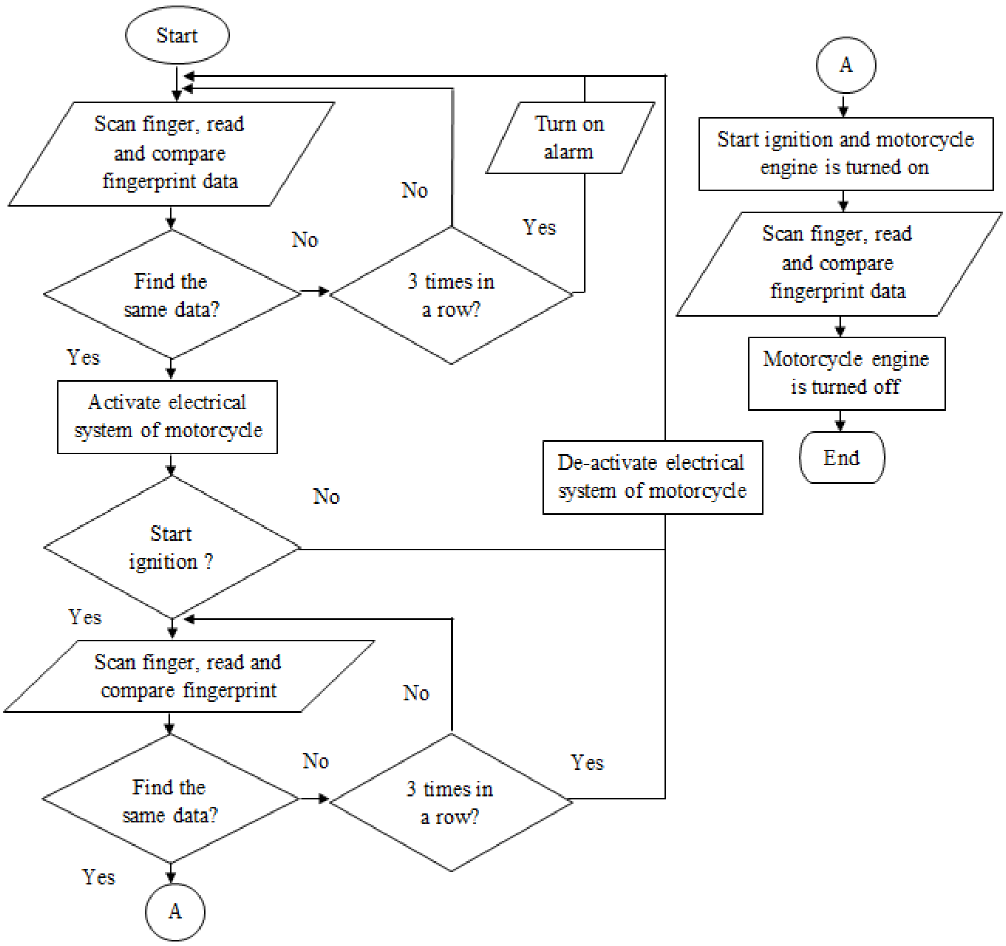


**Figure 6**. Flowchart of overall computational steps of microcontroller

For data processing, the first step is obtaining fingerprint image data through the fingerprint sensor. Then, the fingerprint sensor checks the compliance of fingerprint data with fingerprints stored in the database prior to the data send to the microcontroller. If the microcontroller receives matched data then it generates a command to the relay 1 to activate the electrical system, however, if the microcontroller does not receive matched data for three attempts of the fingerprint scan in a row, the microcontroller generates a signal to turn on the alarm.

As a prototype, the alarm will on and off maximum five times with a period of 100 milliseconds. The part of the program used to check fingerprint data and turn on the alarm can be seen in **Figure 7**. After the electrical system is active, if the user would like to ignite the engine, the user must rescan the fingerprint. The microcontroller will check the re-scanned fingerprint to the previous one. If it was compliance, the microcontroller generates a command signal to relay 2 to start the engine. Nevertheless, if within five seconds after the electrical system has been activated but the user does not rescan the fingerprint, the electrical system will be turned off automatically and the process must be started from the beginning. When the engine is running, if the user wants to turn off the engine, the user needs to re-scan his/her fingerprint again, so that the microcontroller will send a command signal to turn off the relay 2 which is connected to the electrical system, so that the engine will be turned off.

```
int getFingerprintIDez() {
  uint8_t p = finger.getImage();
  if (p != FINGERPRINT_OK) return -1;

  p = finger.image2Tz();
  if (p != FINGERPRINT_OK) return -1;

  p = finger.fingerFastSearch();
  if (p != FINGERPRINT_OK) {
    for(int d=1;d<=5;d++)
  {
    digitalWrite(buzzer,LOW);
    delay(100);
    digitalWrite(buzzer,HIGH);
    delay(100);
  }
  p=0;
   while (p != FINGERPRINT_NOFINGER) {
     p = finger.getImage();
    }
   //..................................
      return -1;}
```

**Figure 7.** Part of program for checking fingerprint data and turn on the alarm

## 3. Result and Discussion

### 3.1. Implementation of proposed system

The proposed fingerprint-based ignition key was implemented on Honda New Megapro (KC21E), a four-stroke motorcycle that still uses a mechanical key for engine ignition. The motorcycle was using a direct current (DC) ignition system. **Figure 8** shows the placement of the fingerprint sensor, the on/off switch, and the plastic box containing the hardware circuit. The SEN0188 fingerprint sensor and the on/off switch were placed on the right-hand side of the motorcycle body so that it was easy to reach by the user while the plastic box containing hardware circuit was placed inside the motor body under the seat so that it was protected from a knock, shock, water, and other hazards.

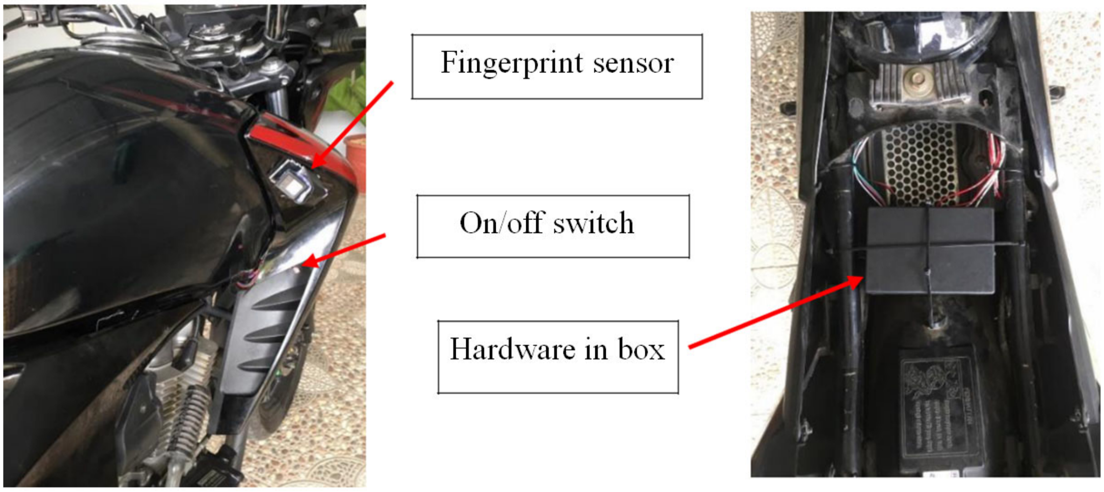


**Figure 8**. The placement of fingerprint sensor, on/off switch, and box of hardware circuit on a motorcycle.

### 3.2. Voltage regulator performance testing

The performance of the voltage regulator needs to be known because it acts as the main power source for the microcontroller. If the voltage and current produced are higher than what is needed, it will damage the component due to the overheat. Measurements were made using a multimeter, where all hardware was installed on the motorcycle. The result of the voltage regulator output voltage measurement is shown in **Table 1**.

**Table 1**. Voltage measurement result before stepped down ($V_{in}$) and after stepped down ($V_{out}$)

| Measurement condition | $V_{in}$ (V) | $V_{out}$ (V) |
|---|---|---|
| Engine was turned off | 12.76 | 9.10 |

In **Table 1**, the voltage before being stepped down is the actual voltage measured from the motorcycle battery output before entering into the voltage regulator circuit while the voltage after being stepped down is the voltage regulator output voltage. The measurement results showed that the output voltage was 9.10 DCV which met the technical specification of the microcontroller. Measurements were then carried out continuously for five minutes with the motorcycle engine running to find out the output voltage profile during the operational condition of the fingerprint-based key. The measurement results presented in **Table 2** showed that the voltage regulator output was 9 DCV with a tolerance of below 0.1 V or 1.1%.

**Table 2**. Voltage measurement result of voltage regulator output in the duration of five minutes

| Measurement condition | $V_{out}$ (V) at i-th minute | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| Engine was running | 9.1 | 9.0 | 9.05 | 8.98 | 9.08 |

In addition to the output voltage measurement, output current measurement profile was also needed because the microcontroller and other instruments have current technical specifications typically between 15 mA and 130 mA. **Table 3** shows the results of measurement of voltage regulator current output when the engine was turned off where the current output was 0.09 A (90 mA). Then, **Table 4** shows measurement results that were conducted continuously for the duration of five minutes in the condition that the motorcycle engine was running where the current output was between 0.15 and 0.18 A or 0.166 A (166 mA) on average. The measurement results showed that the current profile of voltage regulator output has been successfully reduced stable enough to supply current to the microcontroller.

Table 3. Current measurement result before stepped down ($I_{in}$) and after stepped down ($I_{out}$)

| Measurement condition | $I_{in}$ | $I_{out}$ |
|---|---|---|
| Engine was turned off | 1.68 | 0.09 |

**Table 4**. Current measurement result of voltage regulator output in the duration of five minutes

| Measurement condition | $I_{out}$ (A) at i-th minute | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| Engine was running | 0.16 | 0.18 | 0.15 | 0.17 | 0.17 |

The measurement results of voltage and current output of the voltage regulator both when the motorcycle engine was off and on showed that the designed voltage regulator was able to work stably as required.

### 3.3. Fingerprint registration testing

Testing was done by registering the fingerprints of each user. The test was carried out in the condition that the user's fingerprint was dry and clean so that all cross-sections of the finger were not covered and not damaged. One user can register one or more fingerprints. Each registered fingerprint will be given an ID number. Table 5 shows the results of registering five fingerprints of the right hand by one user. If the user registered five fingerprints, the user will be able to turn on and turn off the engine with one of the registered fingerprints but does not need the same fingerprint to turn on and turn off. For example, the user who turns on the motorcycle engine using the thumb can turn it off with the thumb or index finger or other registered fingerprints.

Table 5. Fingerprint registration testing result

| ID No. | Finger | | | | |
|---|---|---|---|---|---|
| | Thumb | Index finger | Middle finger | Ring finger | Little finger |
| 1 | ✓ | - | - | - | - |
| 2 | - | ✓ | - | - | - |
| 3 | - | - | ✓ | - | - |
| 4 | - | - | - | ✓ | - |
| 5 | - | - | - | - | ✓ |

After the fingerprint sensor success to save the fingerprint data of the prospective user, the ignition test was carried out to determine the performance of the developed prototype. To find out the performance on actual condition, the tests were carried out on four different conditions, namely indoor, outdoor, when the fingers are exposed to water/oily/dirty, and on the condition of the motorcycle exposed shocks.

Each condition has different kinds of obstacles. The indoor environmental condition has an obstacle in that it is not bright enough or the presence of lighting that may interfere with the performance of the fingerprint sensor. The outdoor environmental condition especially in the open space without roof/shade has an obstacle in the form of sunlight that potentially interferes with the performance of the fingerprint sensor. Testing for fingerprints that are exposed to water/oily/dirty was done because in daily life the user probably turns on the motorcycle after finishing certain activities that make hands become wet or exposed to oil or exposed to dirt. Testing when there were shakes done because the road conditions are not always smooth but sometimes there are holes or bumps which cause shocks to the motor even though there were suspensions. The success rate of turn on the motorcycle engine can then be calculated using Equation (1). Where, P is the success rate attempts of motorcycle engine ignition in percent, S is the number of successful ignition attempts, and N is the total number of ignition attempts.

$$P = \frac{S}{N} \times 100\% \tag{1}$$

### 3.4. Ignition testing in indoor and shaded area

Testing in an indoor environment was carried out in the garage during the day with lighting only coming from sunlight. The test was repeated five times using five registered fingerprints which results are shown in **Table 6**.

**Table 6**. Ignition testing results in indoor environment and shaded area

| No. | Finger | | | | |
|---|---|---|---|---|---|
| | Thumb | Index finger | Middle finger | Ring finger | Little finger |
| 1 | Success | Fail | Success | Success | Success |
| 2 | Success | Success | Success | Fail | Fail |
| 3 | Fail | Success | Fail | Fail | Success |
| 4 | Success | Fail | Success | Sucess | Fail |
| 5 | Success | Fail | Success | Fail | Fail |

By using Equation (1), the test success rate in Table 6 was 80% for the thumb and middle finger while for the index finger, ring finger, and little finger the success rate was 40%. If the success rate was calculated for all tests, i.e. five fingers for five times of testing (25 tests in total), the success rate was 56%. These results indicated that the performance of the fingerprint sensor in the ignition of the motorcycle engine is stable and reliable enough.

### 3.5. Ignition testing in outdoor environment

Testing in the outdoor environment was carried out during the day with the sun fully shining, in an open place where there were no trees or other objects covering the motorcycle and the fingerprint sensor so that the fingerprint sensor was exposed to the sunlight directly. The tests were repeated five times for five registered fingerprints. The test results are shown in **Table 7**.

**Table 7**. Ignition testing result in outdoor environment

| No. | Finger | | | | |
|---|---|---|---|---|---|
| | Thumb | Index finger | Middle finger | Ring finger | Little finger |
| 1 | Success | Fail | Success | Fail | Fail |
| 2 | Fail | Success | Fail | Success | Fail |
| 3 | Fail | Success | Fail | Fail | Succcess |
| 4 | Success | Fail | Success | Success | Fail |
| 5 | Success | Fail | Success | Success | Fail |

The test success rate calculated using Equation (1) showed that the highest success rate was 60% when using the thumb, middle finger, and ring finger, while the lowest success rate was 20% when the test was done using the little finger. The overall success rate of testing, five times with five fingers (a total of 25 tests), was 48%. Practically, this success rate can be increased by covering or shielding the fingerprint sensor in the time of the scanning process so that the success rate would be the same as the results in the indoor environment.

### 3.6. Ignition testing with fingerprint affected by water, oil and dirt

The test was carried out in a shady place so that the fingerprint sensor is not exposed to the sunlight directly. At the time of the test, the fingerprint was moistened with water or cooking oil or dusted. Tests were carried out repeatedly for five registered fingerprints. The results of five times testing can be seen in Table 8.

The test results in Table 8 showed that the highest success rate was 60% achieved by using the thumb while when using the other four fingers the success rates were between 20% and 40%. The overall success rate for 25 tests was 36%. From these results, it can be recommended that users should clean their hands/fingers before turning on/off the motorcycle engine. In addition, when there were failed attempts for three consecutive times and more such as when using the middle finger and little finger then the microcontroller generated signal for turning on the alarm.

**Table 8**. Ignition testing result with fingerprint affected by water, oil and dirt

| No. | Finger | | | | |
|---|---|---|---|---|---|
| | Thumb | Index finger | Middle finger | Ring finger | Little finger |
| 1 | Fail | Success | Fail | Success | Fail |
| 2 | Fail | Fail | Fail | Fail | Fail |
| 3 | Success | Success | Fail/alarm on | Fail | Fail/alarm on |
| 4 | Success | Fail | Fail/alarm on | Success | Success |
| 5 | Success | Fail | Success | Fail | Fail |

### 3.7. Whole systems performance testing when hit by shock

This test was carried out by turning on the motorcycle engine and then drove it through bumpy, potholes and uneven roads so that the motorcycle got shocks. This test was carried out to determine whether there was a broken hardware component or dislodged connection caused by the shock. The motorcycle was also driven through the streets in puddles to find out whether the on/off switch and fingerprint sensor was still functioning well after being splashed by water and through dusty roads to find out whether the proposed fingerprint-based key system was interrupted by the dust. The test results which were conducted repeatedly showed that all hardware components and their connection were in good condition or nothing was broken. Water and dust splashes attached to the fingerprint sensor could be cleaned and the fingerprint sensor can be used normally again.

### 3.8. Comparison with several previous studies

The comparison of proposed systems to other published research results is presented in **Table 9**. Compared to other published works, the proposed system is the simplest system. Apart from the microcontroller, the proposed system used the most minimum instrument and module involving a fingerprint sensor, relay, and alarm module compared to other research results which used more additional modules such as GSM, GPS, Dual Tone Multi-Frequency (DTMF), Bluetooth, and RFID. The proposed system is also a complete system and does not require any additional devices compared to other published systems that were integrated into a cellular phone.

From the point of view of the ignition system, the proposed system sent the fingerprint image data from the fingerprint sensor to the microcontroller directly. In this way, it is expected that it would be faster compared to another system that needs a mechanical key along with the keypad code, camera face recognition, or SMS command of GSM networks which highly depend on the quality of the networks [8]. Other systems require a mechanical key with RFID tag reading [10] and application command sent through Bluetooth with fingerprint enabled [22]. Moreover, the proposed system does not need any recurring operational cost compared to the other previous studies which needed extra cost for balance maintenance of GSM networks. However, the proposed system has weaknesses in that it does not have a tracking system to track the location of the motorcycle.

**Table 9.** Comparison of proposed system to other published research results

| Item | Proposed System | System in [7] | System in [8] | System in [9] | System in [10] | System in [22] |
|---|---|---|---|---|---|---|
| Ignition technology | Fingerprint-based ignition, | Mechanical key-based ignition | Mechanical key with keypad code/ SMS/ Face recognition enabled ignition | Mechanical key-based ignition | Mechanical key with RFID tag enabled ignition | Android application command with fingerprint enabled ignition |
| Safeguarding principle | Preventing thieves to be able to turn on motorcycle engine if fingerprint does not matches | Sending SMS notification after there is theft trial and remote engine turning off by using SMS message | Sending SMS notification plus thief's face and remote engine turning off by using SMS message | Sending SMS notification plus thief's face and remote engine turning off by using SMS message | Preventing thieves to be able to turn on motorcycle engine if RFID tag does not matches and SMS notification | Preventing thieves to be able to turn on motorcycle engine if Android application command and fingerprint do not matches |
| Alarm | Alarm will on automatically after three consecutive failed attempts | No | No | Alarm will on after activated by user through SMS | Alarm will on automatically when the RFID tag does not matches | No |
| Position tracking | No | GPS and SMS | GPS and SMS | GPS and SMS | No | No |
| Additional device | No | Cellular phone | Cellular phone | Cellular phone | Cellular phone | Cellular phone |
| Data communication | No | GSM networks | GSM networks | GSM networks | GSM networks | Bluetooth |
| Recurring operational cost | No | Maintenance cost for GSM networks | Maintenance cost for GSM networks | Maintenance cost for GSM networks | Maintenance cost for GSM networks | No |

## 4. Conclusions

Fingerprint-based key system performance testing results showed that the fingerprint sensor was able to store and verify the registered fingerprint data. The results of ignition tests of motorcycle engine using fingerprint in indoor, outdoor, and for wet/oily/dirty fingerprints showed that the highest average success rate was 56% reached by indoor/shaded environment while the lowest was 36% for wet/oily/dirty fingerprints condition. For finger type classification, the highest average success was obtained by using a thumb that was 80% when tested in an indoor/shaded environment while the lowest was 20 % obtained by using the middle finger for wet/oily/dirty condition. The fingerprint-based key system showed stable and reliable performance in the condition of shock when tested on potholes, bumpy and uneven roads. Moreover, the alarm of the lock system succeeded to be turned on when there were three fingerprint scan attempts in a row which did not match the data stored in the database.

Considering that the proposed system still has a relatively low success rate, this research can be improved in the use of fingerprint sensors that have better accuracy or develop algorithms in microcontrollers to improve the accuracy of fingerprint image readings. In addition, future work must consider the type of motorcycle ignition. Also, its effectiveness and efficiency must be compared with RFID based keys known as immobilizer which are now widely used as standard locking systems for motorbikes and cars today.

## Author's declaration

**Authors' contributions and responsibilities**

√ The authors made substantial contributions to the conception and design of the study.

√ The authors took responsibility for data analysis, interpretation and discussion of results.

√ The authors read and approved the final manuscript.

**Funding**

No funding information available from the authors.

**Availability of data and materials**

√ All data are available from the authors.

**Competing interests**

√ The authors declare no competing interest.

## References

[1] BPS, "Crime Statistic 2019," Statistics Indonesia, 2019. [Online]. Available: https://www.bps.go.id/publication/2019/12/12/66c0114edb7517a33063871f/statistik-kriminal-2019.html.

[2] U. A. Ojedokun and E. A. Ogundipe, "Motorcycle theft victimization in Oyo town, Nigeria: A qualitative analysis," International Journal of Criminal Justice Sciences, vol. 12, no. 1, pp. 45–56, 2017.

[3] D. J. Barrera et al., “Motor Vehicle Theft in Negros Oriental Philippines: Patterns Across Space, Time, and Targets,” Prism, vol. 20, no. December, pp. 1–16, 2015.

[4] Z. A. Ghani, “A comparative study of urban crime between Malaysia and Nigeria,” Journal of Urban Management, vol. 6, no. 1, pp. 19–29, 2017.

[5] R. M. Susanto, T. Nurrochman, S. Munahar, and A. I. Ramadhan, “Design and Application of Electronic Tracking Control Systems (ETCS) to Improve Vehicle Safety,” Automotive Experiences, vol. 2, no. 3, pp. 67-72, 2019.

[6] H. Fahrian, S. Munahar, and D. S. Putra, “Pengembangan Sirkuit Security System untuk Meningkatkan Driver Behaviour Control pada Kendaraan,” Automotive Experiences, vol. 1, no. 01, pp. 13-19, 2018.

[7] P. Singh, T. Sethi, B. B. Biswal, and S. K. Pattanayak, “A Smart Anti-theft System for Vehicle Security,” International Journal of Materials, Mechanics and Manufacturing, vol. 3, no. 4, pp. 249-254, November 2015.

[8] Y. D. Austria, L. L. Lacatan, J. G. D. Funtera, S. C. Garcia, J. H. Montenegro, and L. T. Santelices, “Face recognition for motorcycle engine ignition with messaging system,” International Journal of Computing Sciences Research, vol. 1, no. 3, pp. 38-49, 2017.

[9] A. O. Pachica, D. S. Barsalote, J. M. P. Geraga, J. M. Ong, and M. D. Sajulan, “Motorcycle Theft Prevention and Recovery Security System,” International Journal of Applied Engineering Research, vol. 12, no. 11, pp. 2680-2687, 2017.

[10] W. W. I. Wan Jusoh, K. A. Mohd Annuar, S. H. Johari, I. M. Saadon, and M. H. Harun, “Motorcycle Security System using GSM and RFID,” Journal of Advanced Research in Applied Mechanics, vol. 16, no. 1, pp. 1-9, 2015.

[11] T. V. D. Putte, and J. Keuning, “Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned,” IFIP CARDIS, 2000, 289-303, 2000.

[12] A. Utzhanova, 2016, “Fingerprint Technology and Sustainable Development,” European Journal of Sustainable Development, vol. 5,no. 4, pp. 325-334, 2016.

[13] A. El-Sisi, “Design and Implementation Biometric Access Control System Using Fingerprint for Restricted Area Based on Gabor Filter,” The International Arab Journal of Information Technology, vol. 8, no. 4, pp. 355-363, October 2011.

[14] S. S. Mudholkar, P. M. Shende, and M. V. Sarode, "Biometrics Authentication Technique For Intrusion Detection Systems Using Fingerprint Recognition," International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), vol.2, no.1, pp. 57-65, February 2012.

[15] J. Kalunga, and S. Tembo, "Development of Fingerprint Biometrics Verification and Vetting Management System," American Journal of Bioinformatics Research, vol. 6, no. 3, pp. 99-112, 2016.

[16] S. G. Eze, and E. O. Chijioke, "Public Enlightenment Education on the acceptance of Fingerprint Biometric Technology for administration in academic institutions and other organizations," Journal of Education and Practice, vol.7, no.28, pp. 158-163, 2016.

[17] Y. H. Jo, S. Y. Jeon, J. H. Im, and M. K. Lee, "Security Analysis and Improvement of Fingerprint Authentication for Smartphones," Mobile Information Systems, vol. 2016, pp. 1-11, 2016.

[18] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, 2019, "Security and Accuracy of Fingerprint-Based Biometrics: A Review," Symmetry, vol. 2019, no. 11, pp. 1-19, 2019.

[19] W. E. Yudiatmaja, T. Samnuzulsari, Alfiandri, and S. Mahdalena, "Fingerprint, Monitoring and Work Discipline of Indonesian Public Servants: Evidence from Kepulauan Riau," Public Administration Research, vol. 7, no. 1, pp. 39-50, 2018.

[20] H. Supriyono, and A. N. Hadi, "Designing a wheeled robot model for flammable gas leakage tracking," In Proceedings of the second International Conference on Informatics and Computing. Jayapura; 2017, pp. 1-6, 2017.

[21] H. Supriyono, E. D. Febriyanto, K. Harismah, "Portable Machine to Machine System for Monitoring Temperature and Flammable Gas of Outdoor Environment," in AIP Conference Proceedings 2114 040014 (2019). Surakarta; 2019, pp. 040014-1- 040014-8, 2019.

[22] M. G. F. Carse, J. V. Custodio, and J. V. S. Verzosa, "Secured Fingerprint-enabled Keyless Motorcycle Authentication System using Arduino," International Journal of Computer Applications, vol. 178, no. 22, pp.19-22, June 2019.